**Hyrje në mjetet e monitorimit të rrjetit**

Për të monitoruar rrjetin analistët e rrjetit përdorin kto mjete monitorimi : **Analizuesit e protokollit** : Janë programe të cilat na mundësojnë kapjen e trafikut deri (wireshark). **NetFlow** : Na ofron informata rreth gjdo IP e cila rrjedh në një paisje. **SIEM** : Sistem i informacionit të eventeve të sigurisë na ofron raportim dhe analiza afat gjate rreth ngjarjeve të sigurisë që ndodhin në rrjetë. **SNMP** : Siguron kërkim dhe mbledhje pasive të informatave për të gjitha paisjet në rrjetë.

**Analizuesit e protokollit** : Na ofrojnë pamje të shkëmbimeve të informatave në rrjet deri në nivel të paketës. Përdoren për të zgjedhur probleme në rrjet, për zhvillim softuerik dhe për edukim.

**Netflow :** Ëshë teknologji e cisco IOS, bën analiz 24/7 të paketave që kalojnë në routerët CISCO, përdoret për ta analizuar trafikun, monitoruar rrjetin dhe planifikuar atë. Nuk e kapë përmbajtien.

**SIEM** : Ofronë funksione themelore si : analiz-mjeko-ligjore, korrelacion, agregim dhe raportim.

**Splunk dhe Elk** janë dy SIEM më të përdoruara nga Qendrat e operimit të sigurisë.

**Sulmet Spmurfing** : Këto sulme përdorin teknikën e amplifikimit dhe reflektimit për ta sulmuar viktimën. Sulmi fillon në momentin kur sulmuesi e dërgon një request ICMP echo me source ip të viktimës drejt një ushtrie të sulmuesve të cilët sulmin e reflektojnë tek viktima për ta tronditur atë.

**HTTP 302** : Mundëson web faqeve ridirektimin në URL tjerë e cila mund të rezultojë në ridirektim tek kode me qëllim të keq.

**Domain shadowing** : Përdoret nga web me qëllim të keq, të cilat ndërtohen në nëndomaina të një domaini tjetër.

Email dërgohen tek shumë paisje në të njëjtën kohë dhe nuk mbrohen nga firewall në të shumtën e rasteve, kjo mundëson realizimin e sulmeve si : **Attached-based-attack** : Nodhë kur në email bashkangjitet një foto ose fajll tjetër i cili është i ekzekutueshëm, dhe ekzektuon kod të keq. **Email-spoofing** : Pranimi i email që duken si legjitime por nuk janë. **Spam Email** : Janë reklama ose email me qëllime të këqija. **Homoglyphs** : Kur Hyperlinks paraqiten si tekste normale.

**Sulmet e injektimi të komandës** : Ndodhin kur injektohen komanda në forma ose në shirita të adresës, kjo shkaku i kodeve të pa sigurta.

**XSS Cross-site scripting attacks** : Janë sulme që realizohen duke injektuar skripta në web të cilat pastaj do bëhen të qasëshme për të gjithë përdoruesit e ati web.

**SQL Injections** : Janë kode SQL të cilat ekzekutohen pa u verifikuar dhe validuar, kto vin zkaonisht nga sulmet e injektimit të komandës.

**Injektimi HTTP** : Kur kodi injektohen duke përdorur tagjet e HTML.